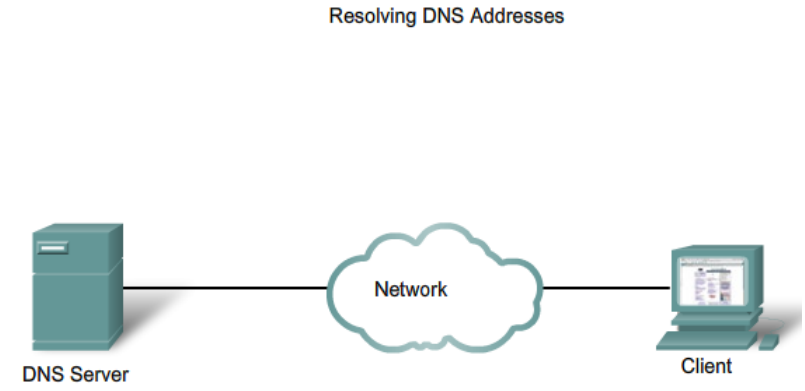
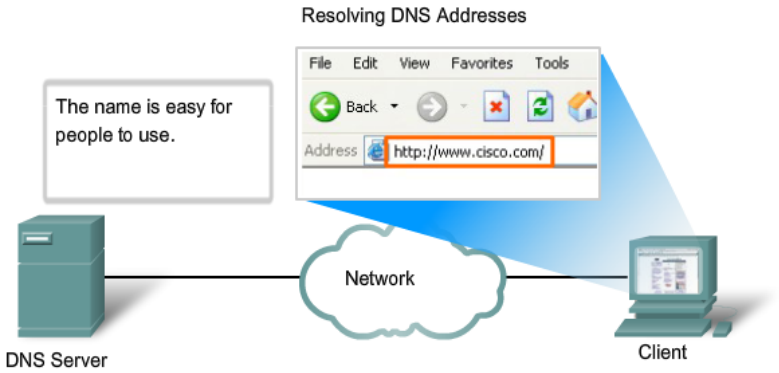
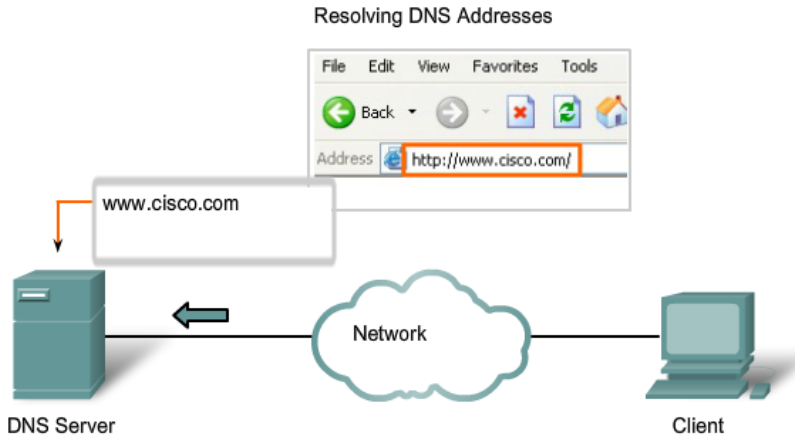
DNS

1. DNS

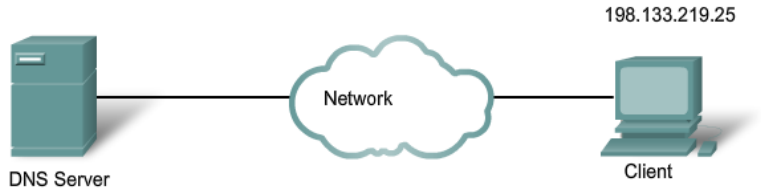
Some figures to remember how DNS works…





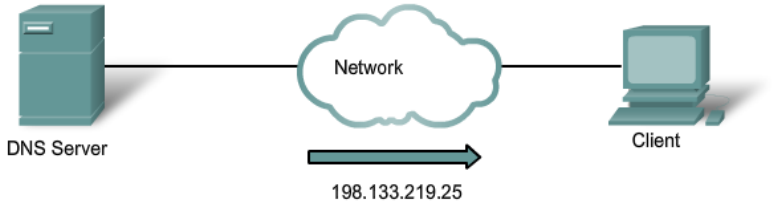


Resolving DNS Addresses



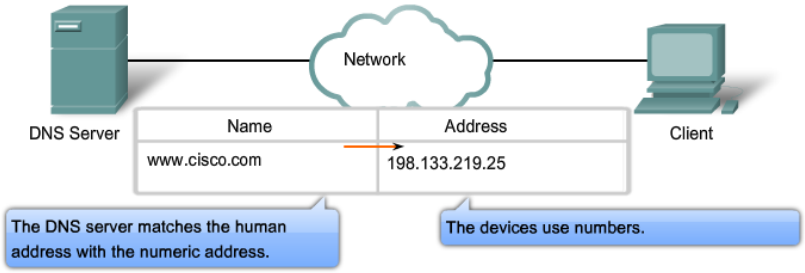
A human legible name is resolved to its numeric network device address by the DNS protocol.

Resolving DNS Addresses

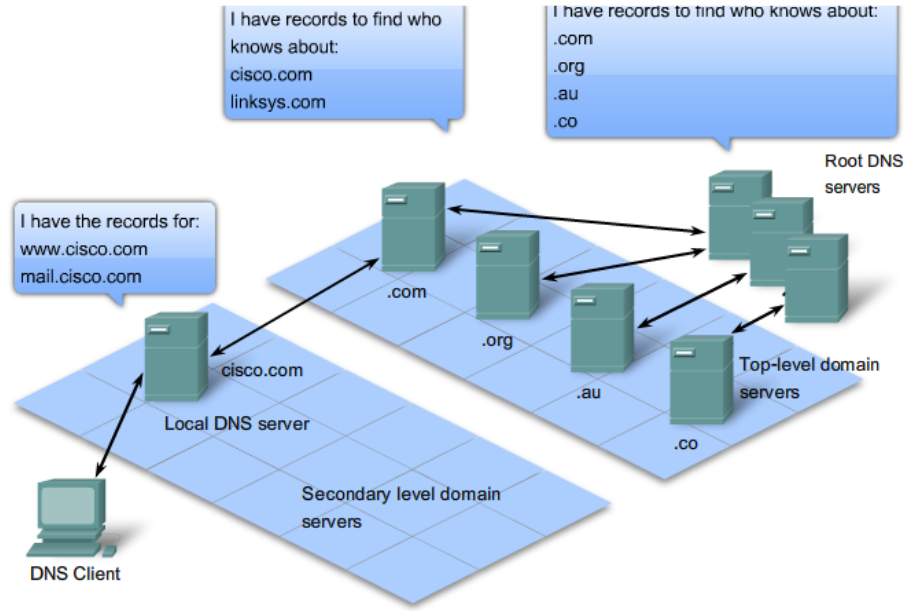


The number is returned back to the client for use in making requests of the server.

Resolving DNS Addresses



The Domain Name System uses a hierarchical system to create a name database to provide name resolution. The hierarchy looks like an inverted tree with the root at the top and branches below. At the top of the hierarchy, the root servers maintain records about how to reach the top-level domain servers, which in turn have records that point to the secondary level domain servers and so on.



A hierarchy of DNS servers contains the resource records that match names with addresses.

1.1. Querying DNS servers

A **DNS server provides the name resolution using the name daemon**, which is often called **named, (pronounced name-dee)**.

The DNS server stores different types of resource records used to resolve names. These records contain the name, address, and type of record.

Some of these record types are:

2. A - an end device address
3. NS - an authoritative name server
4. CNAME - the canonical name (or Fully Qualified Domain Name) for an alias; used when multiple services have the single network address but each service has its own entry in DNS
5. MX - mail exchange record; maps a domain name to a list of mail exchange servers for that domain

Each host has a defined list of DNS servers to contact. On Unix / Linux and MacOS systems the list is found in the file **/etc/resolv.conf**. In Windows it is possible to define the list of DNS servers in the network properties. This list is defined manually (typically on servers with static IP addresses) or automatically after a response from the DHCP server.

Commands to resolve domain names

[HOST]

```
host www.google.com
www.google.com has address 216.58.215.132
www.google.com has IPv6 address 2a00:1450:4003:801::2004
```

[NSLOOKUP]

```
nslookup
> www.google.com
Server:         192.168.1.254
Address:  192.168.1.254#53
```

(Domain name to search)
(DNS Server contacted)

```
Non-authoritative answer:
Name:    www.google.com
Address: 172.217.17.4
```

(DNS server answer – Non- authoritative means that the server 192.168.1.254 does not know the name but it gets the answer after contacting other DNS servers)

```
nslookup www.sapo.pt
Server:         192.168.1.254
Address:  192.168.1.254#53

Non-authoritative answer:
Name:    www.sapo.pt
Address: 213.13.146.142
```

```
nslookup
> set type=MX
```

(Search for MX records (SMTP server for a given domain)

```
> estg.ipp.pt
Server:         192.168.1.254
Address:  192.168.1.254#53
```

(Domain name to search)
(DNS Server contacted)

```
Non-authoritative answer:
estg.ipp.pt   mail exchanger = 0 estg-ipp-
pt.mail.protection.outlook.com.
```

(Answer)

```
> set type=A
```

(Set search type as A (domain name <-> IPv4 address)

```
> estg-ipp-pt.mail.protection.outlook.com
Server:         192.168.1.254
Address:  192.168.1.254#53
```

(Hostname to search)

(DNS Server contacted)

```
Non-authoritative answer:
Name: estg-ipp-pt.mail.protection.outlook.com
Address: 104.47.2.36
Name: estg-ipp-pt.mail.protection.outlook.com
Address: 104.47.0.36
```

(Answer)

[DIG]

```
dig www.google.com
```

```
dig www.google.com MX
```

5.1. How do a bind request is processed?

When a client makes a query:

- First it looks to the DNS local cache to see if it can resolve the name;

- If it is unable, then the client contacts the list of DNS servers configured and then the DNS server (named) process looks at its own records to see if it can resolve the name.
    - If it is unable to resolve the name using its stored records, it contacts other servers to resolve the name.
        - The request may be passed along to many servers, which can take extra time and consume bandwidth.
        - Once a match is found and returned to the original requesting server, the server temporarily stores the numbered address that matches the name in cache.

If that same name is requested again, the first server can return the address by using the value stored in its name cache. Caching reduces both the DNS query data network traffic and the workloads of servers higher up the hierarchy. The DNS Client service on Windows PCs optimizes the performance of DNS name resolution by storing previously resolved names in memory, as well. The "`ipconfig /displaydns`" command displays all the cached DNS entries on a Windows XP or 2000 computer system. ATTN: This could lead to some problems when a DNS recorded is updated.

The Domain Name System relies on this hierarchy of decentralized servers to store and maintain these resource records. The resource records list domain names that the server can resolve and alternative servers that can also process requests. If a given server has resource records that correspond to its level in the domain hierarchy, it is said to be authoritative for those records.